ALL APPLICATION MATERIALS MAILED EXPRESS MAIL CERTIFICATE EK441062442US ON DECEMBER 1, 2000

FORM PTO-1390 (REV 10-2000) — U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
400-101	
U S APPLICATION NO (If known, see 37 CFR 1 5)	
09/701790	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/03839	June 2, 1999	June 3, 1998

TITLE OF INVENTION
METHOD FOR SECURED ACCESS TO DATA IN A NETWORK

APPLICANT(S) FOR DO/EO/US
Paul Pere

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).
4. [X] The US has been elected by the expiration of 19 months from the priority date (PCT Article 31). *
5. [ ] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 16 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    (see page 3 for continuation)

* A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

PCT/PTO 01 DEC 2000

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/701790	PCT/EP99/03839	400-101

17. [X] The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

	CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	

ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 860	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE	
Total claims	24	- 20 =	4	X **$18.00**	$ 72
Independent claims	1	- 3 =	0	X **$80.00**	$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ **$270.00**	$ 270
TOTAL OF ABOVE CALCULATIONS =					$ 1202
[X] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.					$ 601
SUBTOTAL =					$ 601
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					$
TOTAL NATIONAL FEE =					$ 601
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +					$
TOTAL FEES ENCLOSED =					$ 601
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $ 601 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [ ] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. _____. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

Elliott N. KRamsky, ESq.
LAW OFFICES OF ELLIOTT N. KRAMSKY
5850 Canoga Avenue, Suite 400
Woodland Hills CA 91367
Ph: (818) 992-5221
Fx: (818) 710-2751

SIGNATURE:

Elliott N. Kramsky
NAME

27,812
REGISTRATION NUMBER

Method for secured access to data in a network

The invention relates to a method for secured access to data in a network, specifically in a network with an information center and at least one data area access system, the term data area access system being understood as meaning a device which provides storage space (data area) and permits access to stored data.

In the near future, so-called "networks of practices" are to be developed for different interest groups of a public or private sector, for example in health care, for instance for sickness insurance agencies, the health ministry and medical associations. The basic idea of these networks of practices is that, on the basis of better communication between different doctors' practices and/or hospitals, the number of often redundant medical examinations currently still being carried out can be reduced. As an example of this, it would not be necessary to produce a further X-ray image of a lung of a patient if renewed diagnosis, for example by a different doctor, were possible with the assistance of an easily accessible, recently taken X-ray image of this patient's lung. It is in the public interest and the interest of insurance companies to reduce health costs, for which reason the latter in particular would like to set up autonomous medical networks with the aid of which different doctors of a patient can also access this patient's data already prepared by their colleagues, to provide a patient with better and more cost-effective medical care.

In test models already set up, the main problem is that of ensuring secure communication. There are different known ways of connecting a doctor to medical units, which are mainly restricted to a certain group of doctors, for example radiologists, with a restriction to a specific type of information/data, for example X-ray plates, being prescribed of course.

Some national and international standards which define the way in which medical data are generated and transmitted already exist, for example DICOM for X-ray plates, BDT for the data of a patient, GDT for medical data generated by medical equipment, for example by an electrocardiograph or other devices. No special requirements have to be met in these cases with regard to the secured transmission of medical data, since this is no longer a problem today on account of various known encryption mechanisms.

One particular task in the transmission of medical data is to safeguard the individual personal rights of the patient. Nowadays, the transmission of medical information is always illegal whenever it is not restricted to a closed medical group, such as for example a hospital or a doctor's practice. To describe a network of practices with hundreds of different practices and hospitals as a closed group would probably have to be interpreted in the legal sense as an evasion of the personal rights of patients. In this case, a patient would have no possibility of knowing all the members of the group and could scarcely make use of his right to select a different group, such as for example a different hospital.

The invention is accordingly based on the object of specifying a method for secured access to data in a network, in which only the owner of the rights to the data can have free access to these data.

Such a method is specified in patent claim 1. Advantageous developments of this method are to be found in the dependent patent claims 2 to 24.

The method according to the invention provides that only the owner of the rights to certain data can define access rights to these data. Once stored, the data remain where they are stored and are not gathered at a

central location. Access to such stored data is possible only with the authorization of the owner of the rights to these data. For medical data, this means, for example, that they remain at the place where they are prepared and that other doctors can access these data only with the permission of the respective patient. Such permission can be granted generally for certain doctors or else granted only for the individual case.

It is also possible to withdraw permission again once it has been granted.

The invention and advantageous developments are explained in more detail below on the basis of an example with reference to the drawings, in which:

Figure 1 shows by way of example a setup of a network in which the method according to the invention can be used;

Figure 2 shows the generation and storage of data by the method according to the invention;

Figure 3 shows an example of an unsuccessful request for certain data;

Figure 4 shows the retrieval and granting of access rights to certain data by the owner of the rights to these data;

Figure 5 shows an example of a successful request for data and their transmission to the requesting location.

The method according to the invention is explained below, taking a network of practices as an example. Here, the system serves for providing a group of doctors with the medical records of their patients.

The system can be accessed by a number of doctors, who must each have access to a data area access system. In addition to these data area access systems, the system has an information center. For the sake of simplicity, in figure 1 this system is shown with only two data area access systems 1, 2, one of which has an identification DRZS1 and the other has an identification DRZS2. Such a data area access system 1, 2 may be set up at the premises of one or more doctors, for example it is shown in figure 1 that the data area access system 2 is set up at a practice of a doctor B and the data area access system 1 is set up at a hospital in which a doctor A has access authorization to it. Each data area access system 1, 2 can communicate via a network 4 with the information center 3 or another data area access system 1, 2.

Each data area access system 1, 2 contains a secure data memory, in which the medical data of patients can be stored. This memory is access-secured by data access being able to take place only by means of the method according to the invention, as a result of which data misuse with data stored in this memory is not possible. Furthermore, it is insured by the method according to the invention that only new data can be stored, that is to say not data which have already been stored in another data area access system 1, 2. Furthermore, both the respective doctor and the patient can communicate independently of each other via the data area access system 1, 2 with the information center 3 or another data area access system 1, 2 connected to the network 4, with only one doctor being able to store data.

In the information center 3, references to the data of the patients and the associated identification information of the patients and doctors are stored at a central location.

The security of the individual data transmissions within this system is insured by means of an encryption of the data transmissions between all participants. This involves each item of information transmitted within the system being provided with a digital signature. In the case of every access, authorization is demanded, and all data are transmitted and stored in encrypted form. Each participant, for example a doctor or a patient, as well as the information center, and each data area access system have two pairs of public and secret codes for data encoding. One pair of these codes, known as the encryption codes, is used for the secure data transmission and the other, that is the signature codes, provides the transmitted information with a digital signature, and thereby confirms the sender. The secret codes are known only to the respective participant, information center or data area access system, whereas the public codes are accessible to all participants, i.e. every participant in the system has the possibility of obtaining a public code of any other participant. Whenever a participant sends an item of information over the network, the following method is carried out:

1. The sender provides the item of information sent by him with a digital signature, by using his secret signature code. As a result, the sender cannot be imitated, with the recipient being able with the aid of the public signature code to confirm a digital signature used. If, for example, a data area access system sends the information on a patient to the information center, this information must likewise be provided with the secret signature code of this patient when the data are generated. This makes sure that the information really does belong to the patient named, and that this patient agrees to the transmission of this information.

2. The sender encrypts all transmitted data by means of a public encryption code of the recipient to whom the data are being transmitted. As a result, these transmitted data can be decrypted only using the secret encryption code of the recipient.

3. Whenever a participant accesses the system, he must be authorized and have confirmed his identity. A special data carrier, such as for example a smart card, may serve for transmitting the identity of the participant. Of course, other methods of personal identification may also be used, such as for example voice recognition, image recognition, the recognition of fingerprints etc., which can each be used individually or in combination.

As a secure memory for the secret codes of a participant and other personal information, a special data carrier, such as for example a smart card, may likewise be used.

The public codes of the participants, of the information center 3 and of the individual data area access systems 1, 2 may be stored, for example, centrally at the information center 3.

Figure 2 shows the generation of data of a patient and the procedure by which these data are made available in the system.

For example, the patient N visits the doctor A on a day X and has a new medical data unit, for example an X-ray image, prepared. If the patient N desires, this data unit can be made available to other doctors over the network of practices. In this case, in a first step S1, the data of the X-ray image to be stored are stored in electronic form, together with an electronic form which contains the type of the data, in the data area access system 1 with the identification DRZS1 of the

doctor A. The type of the data in this case comprises the information that it is an X-ray image of the patient N, which the doctor A took on the day X. It is also possible for the type of the data to comprise only one of these items of information, or for other information to be added, such as for example the identification DRZS1 of the data area access system 1 storing the data. The data of the X-ray image are stored together with the electronic form in the secured data memory of the data area access system 1. The storing of data is only possible with an authorization of the owner of the rights to these data, which purpose may be served, for example, by the patient's smart card.

In a second step S2, the information center 3 is notified by the data area access system 1 that it has new data, that is an X-ray image of the patient N. Such notification may take place either directly after the storage of the new data or at a certain point in time, for example regularly at a certain time of day. It is also possible of course for the information center 3 to send inquiries as to whether new data have been stored to each data area access system 1, 2 at certain points in time.

In a third step S3, the information center 3 registers the presence of the X-ray image of the patient N of the day X with the availability in the data area access system 1 and allocates these data a unique identification, for example NXAX, after which this identification is transmitted with a notifying confirmation from the information center 3 to the data area access system 1. In the data area access system 1, the identification thus allocated is used for the administration of the associated data, in that it is added to these data. It can be insured by an appropriate configuration that data are not replicated in the system. At the latest when the data are

registered by the information center 3, a verification of the authorization for data storage by the patient takes place here. In the case of no authorization, access rights to these data are not granted to any participant.

In Figure 2, and in the subsequent figures, the hollow arrow signifies a transmission of data into the system, that is to say the storage of new data in a data area access system 1, 2, and the normal arrows respectively signify a communication over the network 4, such as for example a request or notifications. It can consequently be seen from figure 2 that, in the system described, the medical data are not copied into the information center 3 but always remain in the data area access system 1 after they have been stored. The information center 3 keeps only the references to these data and never the data themselves. Furthermore, a data transmission via the network 4 is indicated in the figures by means of boxes in which the data respectively transmitted are specified, represented next to normal arrows.

Figure 3 shows the attempt to access data via the network of practices.

On a day Y, the patient N visits a doctor B, who has a data area access system 2 with the identification DRZS2. This doctor B requires for example a current X-ray image of the patient N. Therefore, in a step S4, the doctor sends from his data area access system 2 a request for X-ray images of the patient N to the information center 3. The information center 3 prepares a list of references to all X-ray images of the patient N currently present in the system as a whole, i.e. stored in any of the connected data area access systems and registered by the information center 3. The information center 3 subsequently verifies the access rights to the data shown in this list with

regard to the doctor B from whom the request for X-ray images of the patient N came, and, in a step S5, transmits only the references of the X-ray images of the patient N to which the doctor B has been granted the access rights by the patient N, who in this case is the owner of the rights to his data. Since, in this case, for example, no access rights to his X-ray images have been defined by the patient N, this list is empty. Therefore, the information center 3 sends a message "no data found" to the data area access system 2. The latter outputs this message to the doctor B.

Accordingly, no doctor can identify the presence of the data in the system without access rights of the patient who is the owner of the rights to the stored data. It is only possible to break through this secure system for certain data for which access rights have been specifically defined if the patient N has, for example, given certain doctors in advance general access rights to all his data or to certain data. Even in this case, however, the patient has himself determined who can access his data, that is to say that here, too, his data protection rights have been respected.

Figure 4 represents the definition of access rights of the patient at the information center 3.

In a step S6, the patient N can, for example, retrieve from the information center 3 via the data area access system 2 a list of all his data currently available in the system as a whole. Alternatively, he can also retrieve only a list of certain data. In a step S7, the information center processes this request and sends the respectively requested list to the data area access system 2. The patient N can now define access rights to the data shown by the list. If, for example, he has requested a list of all his X-ray images, he can define that the doctor B and/or any other doctor or a certain group of doctors can access the X-ray image taken on

the day X by the doctor A with the identification NXAX. Such an access right may be for a limited time or an unlimited time. The access right may also be granted in advance for the data available in future. Once the patient N has defined all the desired access rights, he can, in a step S8, bring about an update of the access rights at the information center 3 via the data area access system 2. In a step S9, the information center 3 stores the changes and sends a confirmation back to the data area access system 2.

These access rights may alternatively also be granted at the point in time at which new data are being stored in a data area access system 1, 2. A patient or other owner of rights to data stored in a data area access system 1, 2 can grant access rights from any desired data area access system 1, 2. For example, it would be conceivable for such data area access systems 1, 2 to be installed not only at doctors' practices or hospitals but also in pharmacies, or for access to a network of practices also to be possible via the Internet, whereby every computer capable of being connected to the Internet could become a data area access system or at least an access system which does not provide any storage space. The owner of the rights to data stored in a data area access system 1, 2, that is in this case the patient, is the only person who, on the basis of his authorization and identification, can be shown the access rights by the information center 3 and/or can modify them at the information center 3.

Figure 5 shows the sequence necessary for successfully accessing certain data.

After the access rights to the X-ray image of the patient N taken on the day X by the doctor A, with the identification NXAX, have been defined by the patient N for the doctor B, the doctor B launches a renewed request to the information center, in a step S10, to

specify all references to the X-ray images of the patient N. In a step S11, the information center compiles a list of the references of all the X-ray images of the patient N currently in any of the data area access systems, verifies the access authorizations with regard to the doctor B making the request and selects only the X-ray images which may be accessed by the doctor B, in order to transmit the associated references to the data area access system 2, from which the doctor B has sent the request to the information center. In this case, for example, only the identification NXAX of the X-ray image of the patient N produced on the day X by the doctor A is transmitted together with the memory location/address, in this case the data area access system 1 with the identification DRZS1, to the data area access system 2, which displays this information to the doctor B. The doctor B can consequently see only the references to data to which the patient N has granted access rights to the doctor B. The references may include, for example, the type of the data, in this case an X-ray image, the date of the examination, in this case the day X, the doctor carrying out the examination, in this case the doctor A, the memory location of the data, in this case the data area access system 1 with the identification DRZS1, or else further data. In a step S12, the doctor B selects the X-ray image with the identification NXAX, whereupon the data area access system 2 sends a request of the doctor B for the X-ray image with the identification NXAX to the data area access system with the identification DRZS1, in this case the data area access system 1. In a step S13, the data area access system 1 then sends an inquiry to the information center 3, in order to confirm that the doctor B has the access rights to the X-ray image with the identification NXAX. The information center 3 replies, in a step S14, with a confirmation, whereupon, in a step S15, the data area access system 1 transmits the data of the X-ray image with the identification NXAX to

the data area access system 2. The latter presents the received data of the X-ray image in an acceptable form and/or allows the doctor B to store the data for further processing, such storage having to take place not in the secure memory of the data area access system 2 but on another storage medium, since otherwise the data would be replicated in the system.

Once an authorized person has stored the received data for further processing, this person can of course repeatedly access the stored data. Access via the network of practices is only possible, however, as long as the owner of the rights to these data allows it by the definition of the access rights.

Since the method according to the invention consequently provides that storing of certain data is possible only with the permission of the owner of the rights to these data and retrieval of such data is possible only with the permission of the owner of the rights to these data, the personal rights of a patient, for example, are respected. The system operates in an entirely transparent way for any user, without the individual user having to have any knowledge of the security or transmission processes. The encryption of the data sent has the effect that unauthorized persons cannot "listen in" and the definition of certain access rights for certain data by the owner of the rights has the effect that unauthorized access to these data is not possible.

When the data are transmitted, it is particularly advantageous if the appropriation specified by the owner of the access rights for the transmission of these data in the original data context is transmitted together with these data in the form of an "electronic watermark" and these data are additionally marked visibly as an appropriated copy of the original data.

The method according to the invention for secured access to data in a network can of course also be applied to other non-medical networks, since a system of controlling the distribution of individual data is proposed here. Another area of application is, for example, the distribution of personal data for identification purposes, whereby the transmission of these data, for example between different administrative authorities without a centralized database of individual citizens, can be made more flexible. The system according to the invention has the effect that the citizen concerned has sole power of disposal over his individual data.

Patent claims

1. A method for secured access to data in a network with an information center (3) and a plurality of data area access systems (1, 2), in which method an owner of rights to data to be stored can alone allow the storing of these data and define the access rights of third parties to these data at the information center (3),
wherein
   - the data are in each case stored only once in one of the data area access systems (1, 2) not accessible to the owner of the rights,
   - the information center (3) registers the presence of data of a certain type in each data area access system (1), after which the owner of the rights to the stored data can define at the information center (3) access rights of third parties to the data,
   - after a request of a requesting data area access system (2) for data of a certain type, the information center (3) transmits a list of the data present of this certain type, specifying the data area access system (1) respectively storing these data, to the requesting data area access system (2) for which the access rights of the requesting data area access system (2) correspond to the access rights defined at the information center (3) for these data, and
   - the data of the certain type are transmitted directly by the data area access system (1) storing these data to the requesting data area access system (2) only if the data area access system (1) storing these data has received a confirmation from the information center (3).

2. The method as claimed in claim 1, wherein an authorization of the storage of data and of the definition of the access rights of third parties to

the data takes place by means of an identity check of the owner of the rights to the data.

3. The method as claimed in claim 1 or 2, wherein data to be stored are stored in the data area access system (1) together with an electronic form, which contains the type of the data.

4. The method as claimed in one of claims 1 to 3, wherein a data area access system (1) storing data responds to a request for certain data of a certain type by a requesting data area access system (2) by verifying the access rights through an inquiry to the information center (3) as to whether the requesting data area access system has access rights to the certain data of a certain type.

5. The method as claimed in one of claims 1 to 4, wherein a data area access system (2) receiving certain data of a certain type allows access to the received data only directly after a respective reception of the data.

6. The method as claimed in one of claims 1 to 5, wherein a data area access system (2) itself storing certain data of a certain type grants access to the certain data of a certain type only if a positive verification has taken place through an inquiry to the information center (3) as to whether the data area access system (1) itself storing the certain data of a certain type can show access rights for the certain data of a certain type.

7. The method as claimed in one of claims 1 to 6, wherein the information center (3) is notified by a data area access system (1) having new data about the presence of new data of a certain type, whereupon the information center (3) sends a

notifying confirmation to the data area access system (1) concerned.

8. The method as claimed in one of claims 1 to 7, wherein the data are identified on the basis of an identification which is allocated as a unique identification by the information center (3) and is transmitted by the information center (3) after a registration of new data to the data area access system (1) storing these data, in order for this system to append the respective identification to the respective data.

9. The method as claimed in one of claims 1 to 8, wherein, after an inquiry for data of a certain type by a data area access system (2), the information center (3) prepares a list of all the data present of this certain type before it verifies the access rights to the data of the certain type, in order to transmit the list of data present of this certain type, specifying the data area access system (1) respectively storing these data, to the requesting data area access system (2) for which the requesting data area access system (2) can show the access rights.

10. The method as claimed in one of claims 1 to 9, wherein, when data access is desired by a data area access system (1) to data of a certain type, firstly a request for such data of the certain type is sent to the information center (3).

11. The method as claimed in one of claims 1 to 10, wherein, when data transmission is desired from a data area access system (1) storing data to a requesting data area access system (2), firstly a request for certain data of a certain type is sent by the latter system to the data area access system (1) storing these certain data of a certain type.

12. The method as claimed in one of claims 1 to 11, wherein the data in a data area access system (1, 2) are stored in a secure data memory, no direct access being possible to the data stored therein.

13. The method as claimed in one of claims 1 to 12, wherein the type of the data is determined by their content and/or the owner of the rights to the data.

14. The method as claimed in one of claims 1 to 13, wherein the access rights to stored data can be defined by the owner of the rights to the data at any point in time after their registration at the information center (3) and, after that, can be changed again as desired by a re-definition by the owner of the rights to the data.

15. The method as claimed in one of claims 1 to 14, wherein the access rights to stored data can be granted by the owner of the rights to the data when they are stored in a data area access system (1, 2).

16. The method as claimed in one of claims 1 to 15, wherein the communication between a data area access system (1, 2) and the information center (3) or another data area access system (2, 1) takes place in encrypted form.

17. The method as claimed in claim 16, wherein the sender provides the information sent by him with a digital signature by means of a secret signature code, whereby the recipient can verify the sent information by means of an associated public signature code.

18. The method as claimed in claim 16 or 17, wherein the sender encodes all transmitted data by means of

a public encryption code issued by the recipient, whereby only the recipient can decode the transmitted data by means of a secret encryption code.

19. The method as claimed in one of claims 16 to 18, wherein not only each data area access system (1, 2) and the information center (3) but also each participant has a secret signature code and a secret encryption code and a public signature code and a public encryption code.

20. The method as claimed in claim 19, wherein the secret signature codes and encryption codes and/or public signature codes and encryption codes of a participant are stored on a data carrier, such as for example a smart card.

21. The method as claimed in one of claims 1 to 20, wherein a participant accessing the network must authorize himself and his identity is verified by the information center.

22. The method as claimed in claim 21, wherein the identity of a participant is stored on a data carrier, such as for example a smart card.

23. The method as claimed in one of claims 1 to 22, wherein the permission for storing the data is given by the owner of the rights to the data at the latest when the data are registered at the information center (3), the information center (3) not allowing any subsequent data access to these data without correct authorization.

24. The method as claimed in at least one of the preceding claims, wherein, when the data are transmitted, the appropriation specified by the owner of the access rights for the transmission of

these data in the original data context is transmitted together with these data in the form of an electronic watermark and these data are additionally marked visibly as an appropriated copy of the original data.

Abstract

Method for secured access to data in a network

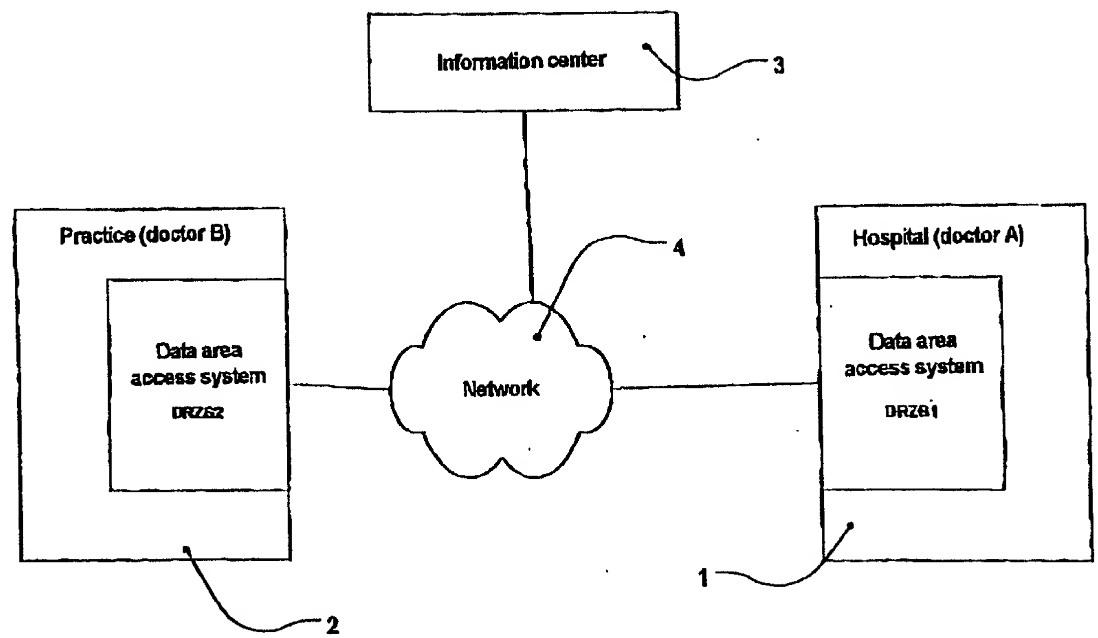
The method according to the invention has the effect that data protection rights are respected, especially with respect to personal data which are available in a network with distributed memories. The method is based on the granting of access rights, with the possibility of revocation, to the data available in the network, and the storage of data within the network only after authorization by the owner of the rights to the data. When certain data are requested, only the references of those data records to which the requesting party also has the access rights can be given, it not being possible without access rights for the data present to be identified. If certain data are to be accessed, the access rights may in turn be verified before data access is allowed.

(Figure 5)

09/701790

1/5

Fig. 1



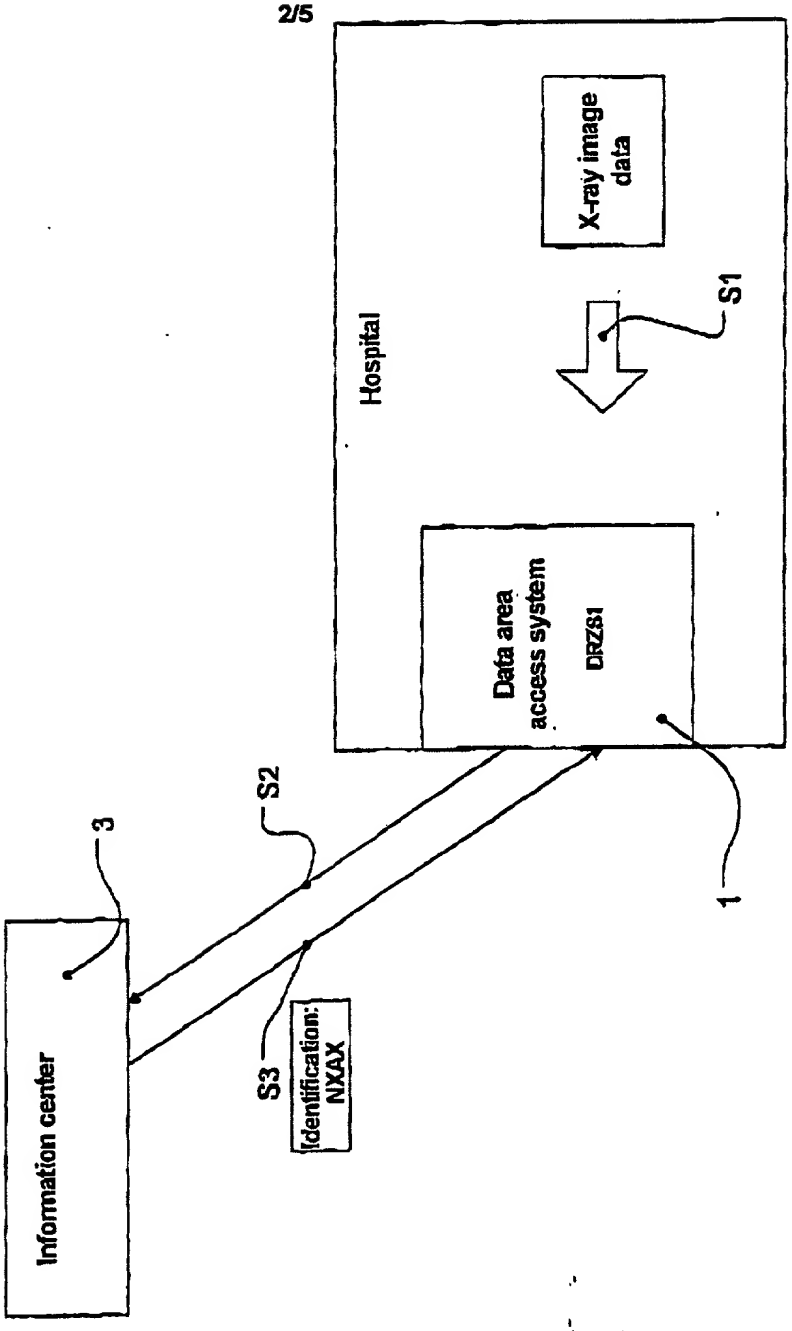

Hospital
X-ray image data
S1
Data area access system
DRZ81
1
S2
3
S3
Identification: NXAX
Information center

Fig. 2

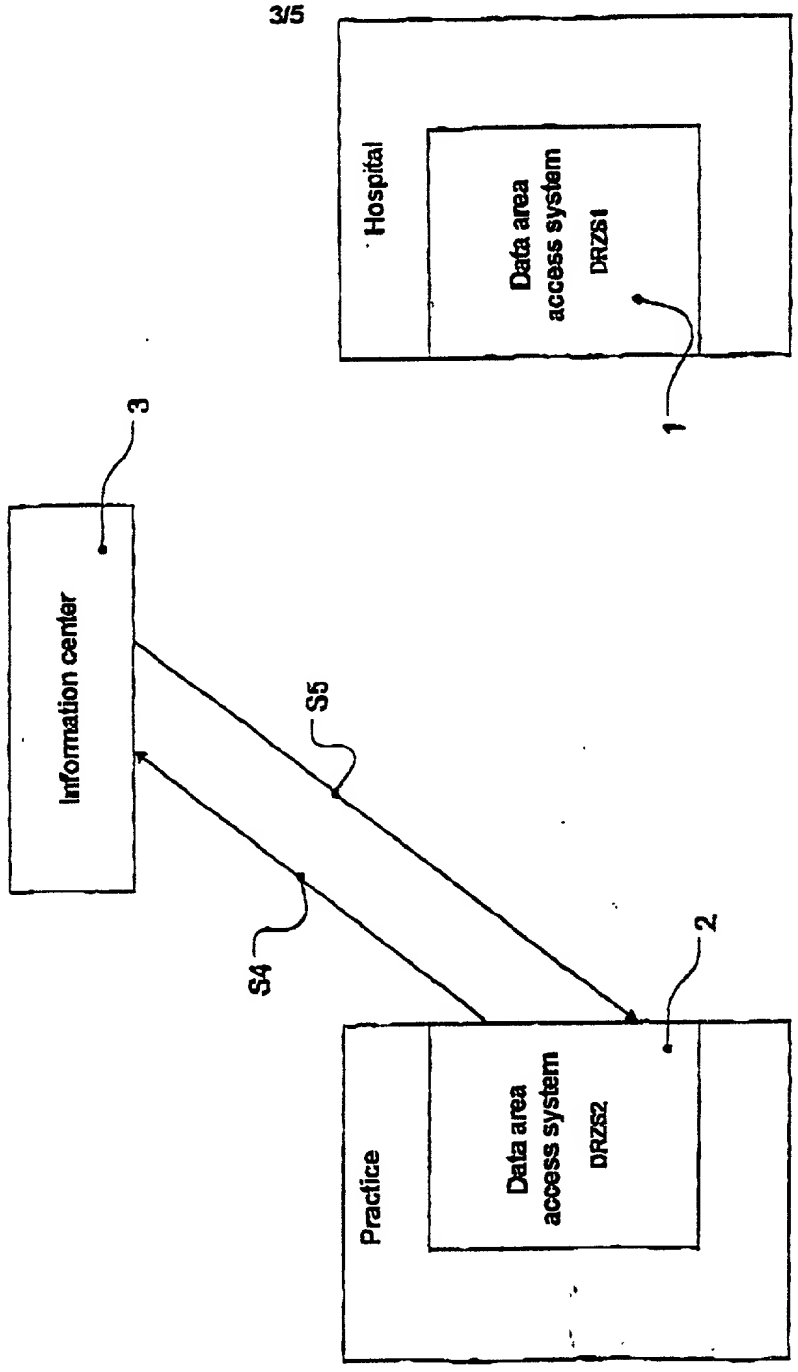
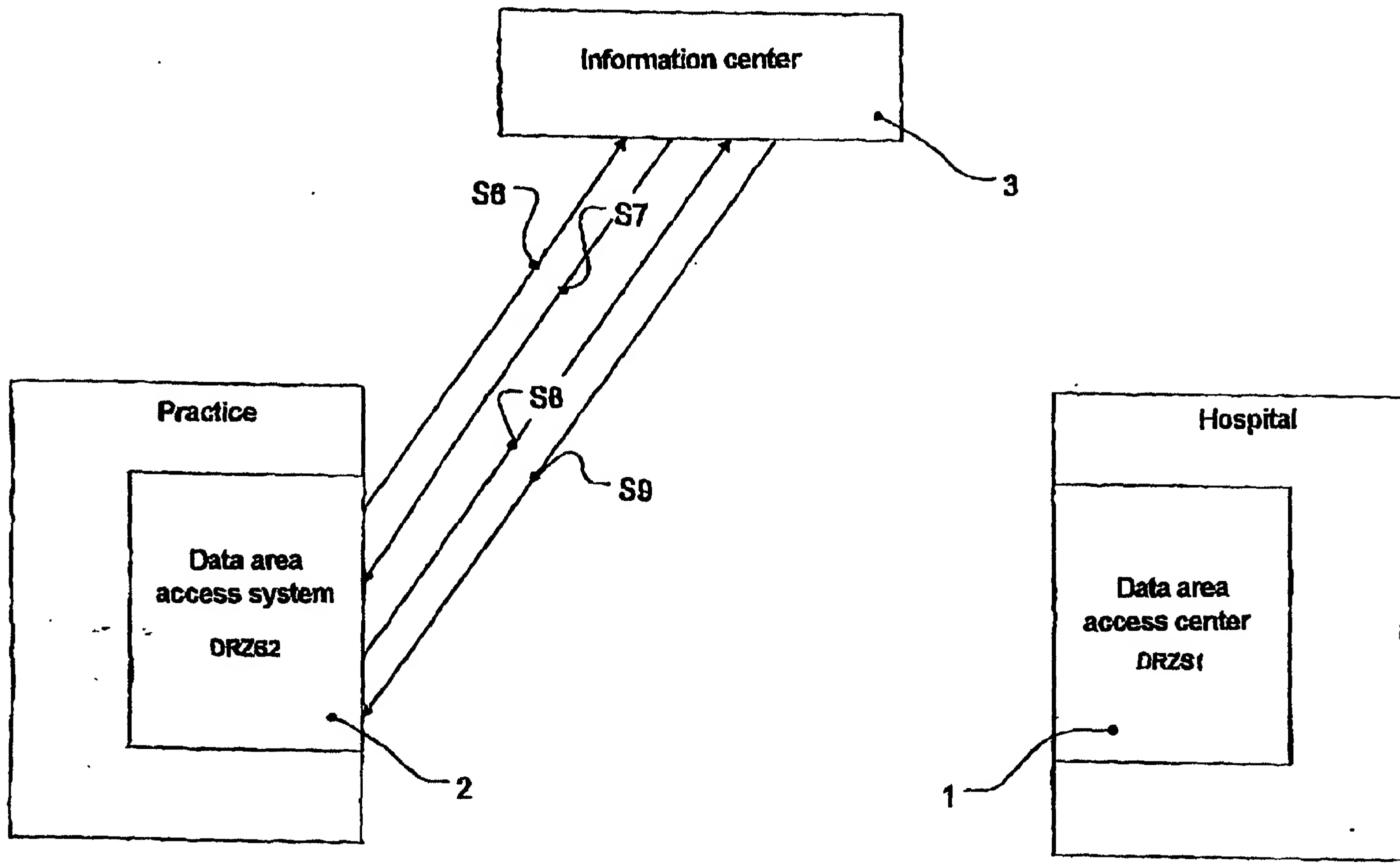

Hospital
Data area access system
DRZS1
1
3
Information center
S5
S4
2
Practice
Data area access system
DRZS2

Fig. 3

Fig. 4



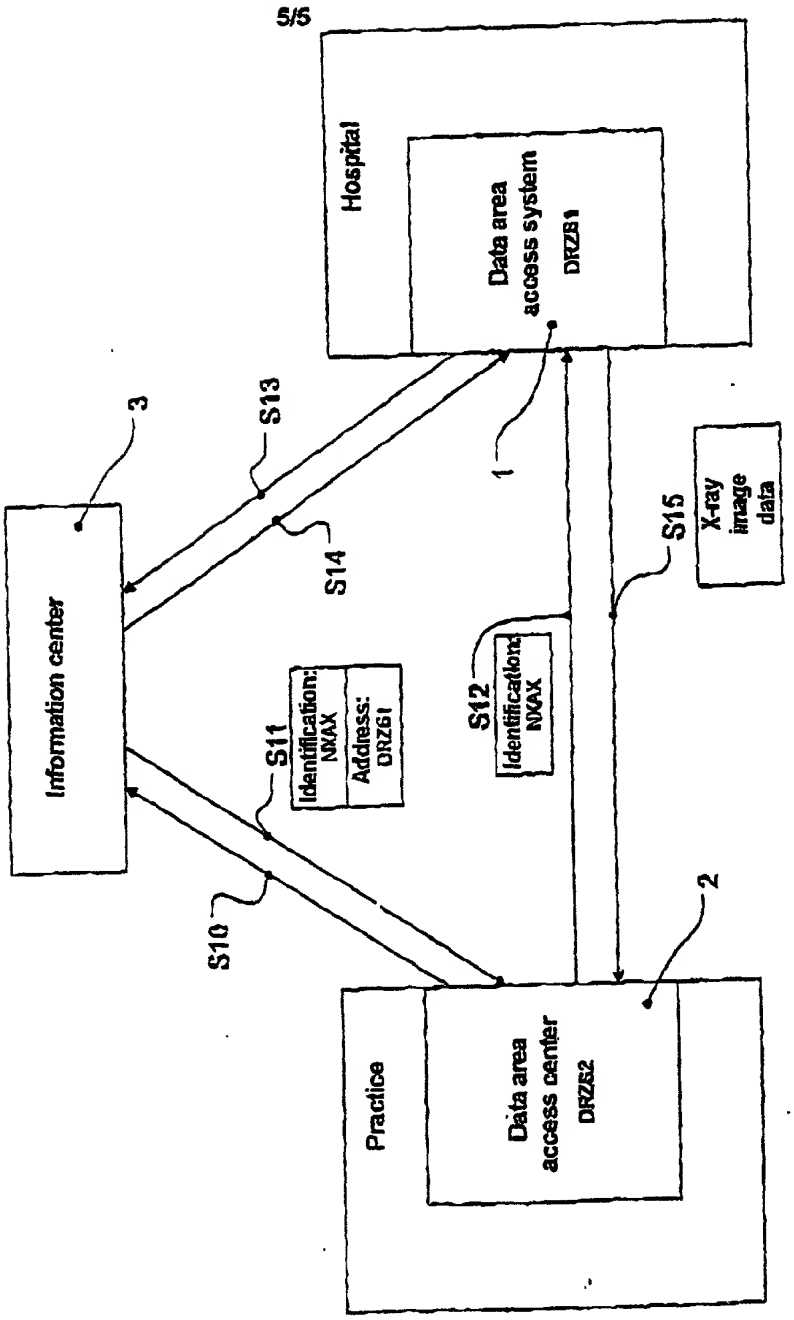

Hospital
Data area access system DRZ61
1
3
S13
S14
Information center
S11
Identification: NXAX
Address: DRZ61
S12
Identification: NXAX
S15
X-ray image data
S10
2
Practice
Data area access center DRZ62

Fig. 5

Docket No. 400-101 (53068)

COMBINED DECLARATION AND POWER OF ATTORNEY

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought, pursuant to the United States national phase of International patent application PCT/EP99/03839 filed June 2, 1999, on the invention entitled METHOD FOR SECURED ACCESS TO DATA IN A NETWORK which is described and claimed in the specification attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German patent application Serial No. 198 24 787.7
Filed: June 3, 1998

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing of the prior application and the national or PCT international filing date of this application: NONE

I hereby appoint ELLIOTT N. KRAMSKY, Registration No. 27,812, my attorney to conduct all business in the Patent and Trademark Office in connection with this application. Please send all correspondence to:

Elliott N. Kramsky, Esq.
5850 Canoga Avenue
Suite 400
Woodland Hills, CA 91367
(818) 992-5221

I hereby declare that all statements made herein of my knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of Inventor: Paul Pere
Name

Germany
Citizenship

Nymphenburger Strasse 92
80636 Munich
Germany
P.O. Address and Residence

Date: 28.11.2000

PAUL PERE